MULTIPLATFORM TEST ENVIRONMENT FOR EFFICIENCY ANALYSIS OF CRYPTOGRAPHIC PRIMITIVES USED IN ELLIPTIC CURVES

Josef Brychta
Master Degree Programme (5), FEEC BUT
E-mail: xbrych07@stud.feec.vutbr.cz

Supervised by: Radek Fujdiak
E-mail: fujdiak@feec.vutbr.cz

Abstract: This paper deals with design of multiplatform test environment for efficiency analysis of cryptographic primitives used in elliptic curves. The test algorithm to generate 1000 random points on the SEC secp256k1 elliptic curve was used on Raspberry Pi 2/3 devices and compared the measured real-time values of the system usage of these devices.

Keywords: Cryptographic primitives, cryptography, elliptic curves, psutil, Raspberry Pi, secp256k1.

1 ÚVOD

Kryptografie je v dnešní době používána prakticky ve všech oblastech, které jakkoliv souvisí s počítači či sítěmi. Od internetového bankovnictví, platebních karet, šifrování souborů, disků nebo jen zabezpečený přístup na webové stránky. Pro usnadnění práce vývojářům byly navrženy různé kryptografické knihovny, které mají za cíl implementovat požadované kryptografické funkcionality. Těchto kryptografických knihoven je spousta a každá je vhodná na jinou platformu [1, 2, 3]. Motivací této práce bylo usnadnění výběru kryptografických knihoven možností vývojářům zjistit reálnou efektivitu počítání kryptografických primitiv těchto knihoven. Sestrojit multiplatformní testovací prostředí pro analýzu efektivity kryptografických primitiv na eliptických křivkách pro různé hardwarové platformy.

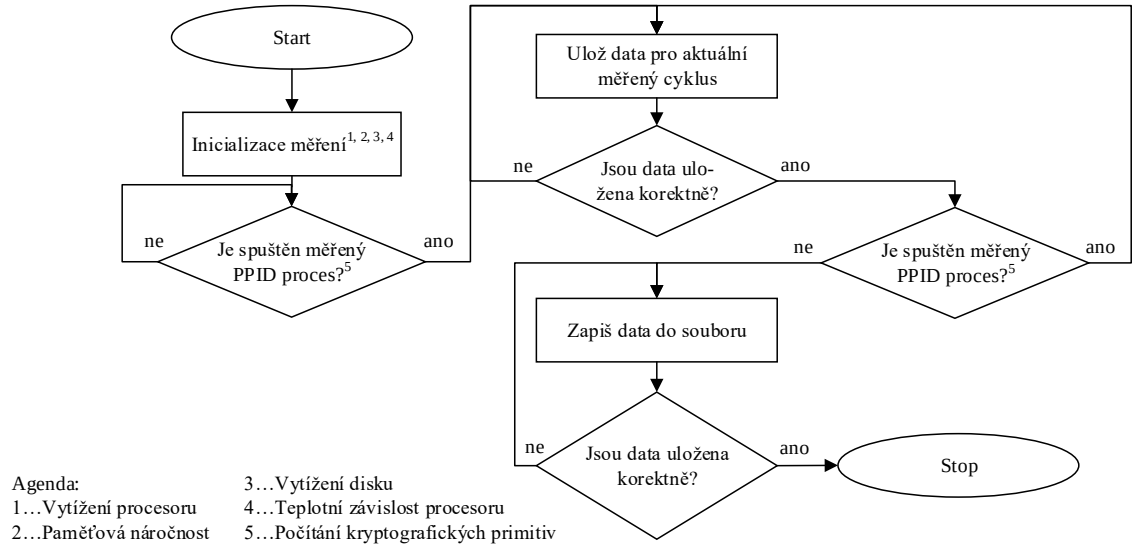
2 ZPŮSOBY MĚŘENÍ EFEKTIVITY KRYPTOGRAFICKÝCH KNIHOVEN

Tato kapitola se zabývá popisem metod, pomocí kterých jsou realizována měření efektivity kryptografických knihoven – počítání kryptografických primitiv s jednotlivými knihovnami. Následující parametry měření jsou realizovány pomocí knihovny psutil a napsány v jazyce Python. Psutil je multiplatformní knihovna pro získávání informací o běžících procesech a využití systému (CPU, RAM, GPU, disky, sítě, čidla) naprogramována v jazyce Python. Je zaměřená primárně na sledování systému, profilování a omezení procesních prostředků a řízení běžících procesů. Implementuje mnoho funkcí nabízených nástroji příkazového řádku systému UNIX, jako jsou: ps, top, lsof, netstat, ifconfig, who, df, kill, free, nice, ionice, iostat, pidof, tty, taskset, pmap.

2.1 POPIS KOMPLEXNÍHO MĚŘÍCÍHO ALGORITMU

Měřící algoritmus obsahuje následující měřící metody: vytížení procesoru, paměťová náročnost, vytížení grafického adaptéru, vytížení disku – ty jsou realizovány pomocí knihovny psutil, která je popsána výše a jsou napsána v jazyce Python. Měřící prostředí čeká s měřením na identifikaci PPID identifikátoru měřené operace v systémových procesech. Neboli po načtení kryptografických knihoven a spuštění výpočetních primitiv těchto knihoven se spustí jednotlivá měření. Měření probíhají v minimálním možném intervalu (procesorových cyklech) pro maximální možnou přesnost měření

v průběhu běhu výpočetních primitiv. Po skončení běhu výpočetních operací se ukončí PPID proces a s ním také měření měřícího algoritmu. Výsledky jednotlivých měření se zapíší do souborů jako hodnoty k následnému zpracování. Vývojový diagram multiplatformního testovacího prostředí pro měření efektivity kryptografických primitiv na eliptických křivkách je znázorněn na Obrázku 1.



Obrázek 1: Diagram multiplatformního testovacího prostředí pro měření efektivity krypt. primitiv.

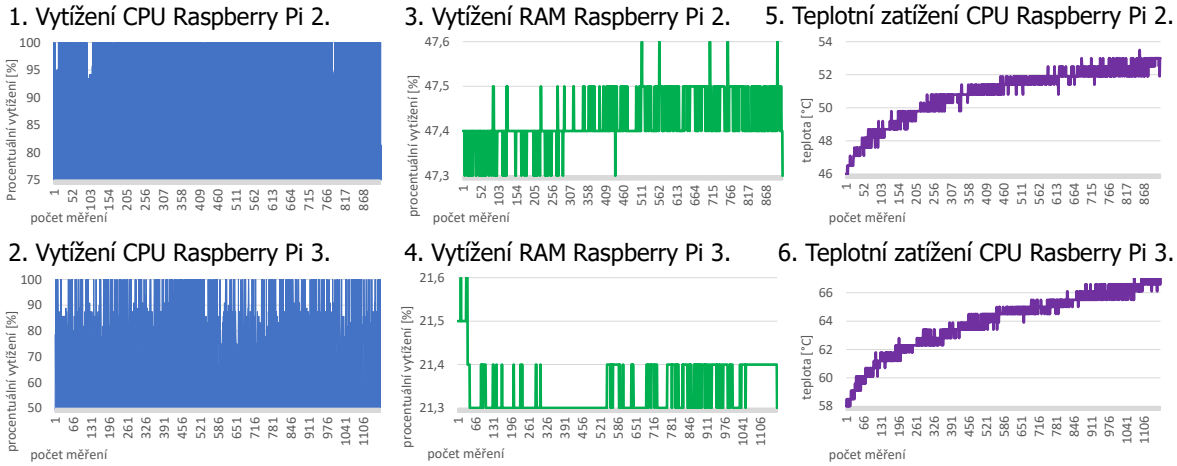
2.2 DALŠÍ MĚŘITELNÉ PARAMETRY

Měření energetická náročnosti je realizováno za pomocí speciální měřícího přístroje citlivého na velmi malé proudy. Další variantou je měření pomocí speciálního přídavného kitu pro Raspberry Pi do I2C sběrnice. Počet strojových cyklů je realizován pouze u projektů, které to umožňují. Například v prostředí Eclipse. Měření časové náročnosti výpočetních operací je realizováno v jazyce Python.

3 MĚŘENÍ NA TESTOVACÍM VÝPOČETNÍM ALGORITMU

Měření probíhalo na dvou zařízeních (Raspberry Pi 2/3). Na obou byl spuštěn skript na vygenerování 1000 náhodných bodů na eliptické křivce secp256k1 ($y^2 = x^3 + 7$) standardu SEC v kryptografické knihovně OpenSSL. Zajímavostí této křivky je, že ji používá ve svém algoritmu Bitcoin. Zařízení Raspberry Pi 2 zvládlo tuto operaci za 38,12 s a Raspberry Pi 3 za 19,37 s. Dalším typem měření bylo procentuální vytížení CPU na jeden procesorový cyklus. Procesor u Raspberry Pi 2 provedl celkem 868 procesorových cyklů. Zatímco procesor u zařízení Raspberry Pi 3 provedl 1106 procesorových cyklů. Z čehož vyplývá, že procesor u Raspberry Pi 2 s taktem 900 MHz na jedno jádro provedl méně cyklů než procesor u Raspberry Pi 3 s taktem 1,2 GHz. Měření vytížení CPU u zařízení Raspberry Pi 2 bylo skoro stále na svém výkonnostním maximu. Je to způsobeno převážně malým výkonem CPU jednotky ARM Cortex-A7 a náročností výpočetního procesu. Na zařízení Raspberry Pi 3 je vidět lepší rozložení výkonu a procesor ARM Cortex-A53 zaměstnává znatelně méně i když se hodnota využití blíží také svému maximu. Dále bylo realizováno měření využití paměti RAM na jeden procesorový cyklus. Nutno podotknout, že testovaná zařízení jsou osazena 1 GB RAM a využití RAM paměti se měnilo pouze v řádu desetin jednotky. Při měření nebyly spuštěny žádné další uživatelské aplikace pro maximální možnou srovnatelnost. Dále bylo realizováno měření procentuálního vytížení paměti FLASH, která nahrazuje u obou zařízení systémový disk. Obě zařízení jsou osazena UHS-I U3 kartou s pamětí 32 GB. Vytížení paměti FLASH při tomto měření bylo konstantní a bylo zjištěno, že

nemá žádný vliv na spuštěné procesy. Proto nejsou přiloženy výsledky tohoto měření. Posledním realizovaným měřením byla teplotní závislosti procesoru na počet procesorových cyklů dané výpočetní operace. Na grafech je vidět, že s časem teplota vzrůstala u obou zařízení ale u Raspberry Pi 3 startovala na vyšší teplotě. Zajímavostí je, že oba procesory u daných zařízení zvýšily svou teplotu o 8 °C. Pro maximální možnou srovnatelnost byla obě zařízení nechána v nečinnosti před samotným měřením. Referenční hodnoty na Raspberry Pi 2 byly: teplota CPU 45,7 °C, vytížení CPU 32,3 % a vytížení RAM 47,3 %. na Raspberry Pi 3 to bylo teplota CPU 57,8 °C, vytížení CPU 15,5 % a vytížení RAM 21,3 %. Výsledky měření vytížení CPU, RAM a teplotní vytížení jsou k dispozici na Obrázku 2.



Obrázek 2: Měření vytížení CPU, RAM a teplotní zatížení na zařízeních Raspberry Pi 2/3.

4 ZÁVĚR

Cílem této práce bylo zrealizovat multiplatformní testovací prostředí pro analýzu efektivity kryptografických primitiv na eliptických křivkách u kryptografických knihoven pro různé hardwarové platformy. Na výše zmíněném testovacím kryptografickém algoritmu byla realizována měření využití CPU, RAM, FLASH a teplotní zatížení na počet jednotek procesorových cyklů daného výpočetního algoritmu na zařízeních Raspberry Pi 2/3. Z výsledků měření je patrné, že Raspberry Pi 3 zvládlo vypočítat měřený kryptografický algoritmus za přibližně polovinu času než Raspberry Pi 2. Raspberry Pi 3 je efektivnější i ve využití systémových prostředků jako jsou CPU i RAM. Rozdíly ve využití maxima výkonu CPU se rapidně liší v závislosti na použitém kryptografickém algoritmu. Navržené měřící prostředí dále umožňuje měření GPU vytížení na procesorový cyklus, měření strojových a procesorových cyklů, čas měření a podrobné nastavení měřených systémových parametrů. Podstatným kritériem pro měření efektivity je také energetická náročnost zařízení, která musí být realizována hardwarově, tj. pomocí přesného multimetru, který umožňuje měřit velmi malé proudy či speciálním doplňkovým měřicím kitem určeným pro zařízení Raspberry Pi 2/3 do I2C sběrnice.

REFERENCE

[1] Bos, W; Halderman, A; Heninger, N a další.: *Elliptic Curve Cryptography in Practice* [online]. 2013, poslední aktualizace 2013. Dostupné z URL: <https://eprint.iacr.org/2013/734.pdf>.

[2] Johnston, O.: *Elliptic Curve Cryptosystems* [online]. 2010, poslední aktualizace 2010. Dostupné z URL: <https://eprint.iacr.org/2010/575.pdf>.

[3] Independent Media.: *Cryptographic Libraries* [online]. 2018, poslední aktualizace 2018 [cit. 9. 03. 2018]. Dostupné z URL: <http://www.tech-faq.com/cryptographic-libraries.html>.